REMARKS

Reconsideration of the pending application is respectfully requested on the basis of the following particulars:

Rejection of claims 1-3, 5-7, 10-21, and 23-26 under 35 U.S.C. § 103(a)

Claims 1-3, 5-7, 10-21, and 23-26 presently stand rejected as being unpatentable over Buffam (U.S. 6,185,316) in view of Matyas et al. (U.S. 6,697,947). This rejection is respectfully traversed for at least the following reasons.

It is respectfully submitted that Buffam and Matyas, either individually or in combination, fail to form a prima facie case of obviousness of the presently claimed invention because these references, taken together, fail to disclose or suggest all of the claim limitations of independent claims 1 and 20, and because there is no motivation or suggestion for any combination or modification of these references to arrive at the presently claimed invention.

Neither Buffam nor Matyas disclose or suggest decrypting an encrypted code word on the basis of a digitized biometric authentication feature data thereby obtaining a decrypted code word, and recovering secret data from the decrypted code word on the basis of a coding-theory method within a freely selectable tolerance level.

Buffam does not disclose or suggest fault-tolerantly coding/decoding of secret data, or the secret data is recovered from the decrypted code word on the basis of a coding theory method within a freely selectable tolerance interval, as the examiner acknowledges in the recent Office action (at page 3).

Buffam does not disclose or suggest decrypting an encrypted code word on the basis of a digitized biometric authentication feature data to obtain a decrypted code word.

Instead of using a digitized biometric authentication feature data to obtain a decrypted code word, Buffam generates ***false minutia*** (not actual biometric data). According to Buffam, "the false minutiae (FIPs) can be hashed to form an encryption key,

step 725." (*Buffam*; col. 20, lines 55-56). The false minutiae (FIPs) are included with (but are not) ***true minutia*** that correspond to a user's fingerprint pattern to form a "transient template" which is stored on a user's credential.

In practice, a claimant "presents credential 605 to credential sensor 615 contemporaneously with providing a live fingerprint scan from fingerprint sensor 614. Thransient template 620 is then extracted from credential 605. From template 620 is extracted candidate [false minutia] vector 635." (*Buffam*; col. 20, line 66 – col. 21, line 3). The user's live fingerprint scan is compared to the ***true minutia*** (TIPs). "If claimant 612 is the same person as represented by the data encoded into credential 605, as determined in comparator 650, the fingerprint scan [***true minutia***] TIPs read in sensor 614 will correspond with the proffered [***true minutia***] TIPs vector from credential 605." (*Buffam*; col. 21, lines 4-8).

After the ***true minutia*** are extracted, "there will remain the set of [***false minutia***] FIPs data 635, which can be hashed in decode key generator 640 to produce decode key 645.

Thus, the decode key 645 is not based on any user biometric data, but is based on the ***false minutia*** which are entirely "made up" data not derived from the actual user biometric data (TIPS or ***true minutia***) at all. Instead, the false minutia are "false image points (FIP) 128 [which] can be created by FIP generator (FIPG) 130, with the FIPs 128 preferably having a substantial degree of entropy, i.e., having a ***highly random content***." (*Buffam*; col. 13, lines 63-66).

Therefore, Buffam does not teach or suggest that an encrypted code word is decrypted on the basis of a digitized biometric feature data, thereby obtaining a decrypted code word.

Moreover, Buffam does not disclose or suggest any error correction at all. Buffam disclose a method in which a list of true and false minutia points is stored, and from which the correct minutia points are extracted during a verification phase, with the aid of a verification template. As noted above, this involves the storing of true and false minutia.

True minutia are evaluated to verify a user, while the false minutia are hashed to produce a decode key. It must be noted that the present invention is not directed to minutia points or any listing of invented (false) minutia points.

Matyas, in contrast to both Buffam and the present invention, discloses a method to combine biometric features of a plurality of users and to authenticate only when the biometric features of a sufficient number of users have been recognized. (see *Matyas*; col. 9, lines 11-14, 24-28).

Thus, Matyas differs from the present invention in that, according to Matyas, authentication is carried out only after the biometric features of a sufficient number of users have been recognized.

Matyas does not disclose or suggest that a secret data is recovered from the decrypted code word on the basis of a coding theory method within a freely selectable tolerance interval.

Matyas discloses that "a secret value, such as a secret key SK, may be determined from shares of the secret value distributed to multiple users." (*Matyas*; col. 15, lines 25-27). However, the secret key is not determined from a decrypted code word, the decrypted code word being obtained by decrypting an encrypted code word on the basis of a digitized biometric authentication feature.

Moreover, because Buffam teaches recovery of a decode key from data other than biometric data (since Buffam recovers the decode key from false minutia, not from actual biometric data), modifying Buffam according to Matyas cannot lead to the present invention.

Even assuming, arguendo, that Matyas discloses that a secret key SK may be obtained from a user's biometric feature by decrypting an encrypted code word on the basis of the biometric authentication feature, and recovering secret data from the decrypted code word on the basis of a coding-theory method within a freely selectable tolerance window, it must be appreciated that Buffam's decode key is contained in the ***false***

minutia, and is therefore not at all related to a user's biometric feature represented by the true minutia.

Since Buffam's true minutia are unrelated to Buffam's decode key, applying Matyas' teachings to Buffam's user biometric data (represented by the true minutia) will not result in extracting the decode key. On the other hand, applying any teachings of Matyas to Buffam's false minutia would not result in secret data obtained by decrypting an encrypted code word on the basis of a digitized biometric authentication feature, because the false minutia are not digitized biometric authentication feature but are instead essentially made-up, random data.

Further, modifying Buffam such that the decode key is extractable from the true minutia would change the principle of operation of Buffam, since Buffam is based on a principle of generating a key from false image points (FIPs, or false minutia) apart from actual biometric data represented as true image points (TIPs, or true minutia).

Therefore, for at least the foregoing reasons, it is respectfully submitted that Buffam and Matyas fail to form a prima facie case of obviousness of the presently claimed invention. Accordingly, it is respectfully submitted that claims 1-26 are allowable over the cited references, and withdrawal of the rejection is requested.

Rejection of claims 4, 8, and 9 under 35 U.S.C. § 103(a)

Claims 4, 8, and 9 presently stand rejected as being unpatentable over Buffam and Matyas in view of Camp Jr. et al. (U.S. 6,075,987). This rejection is respectfully traversed for at least the following reasons.

Claims 4, 8, and 9 depend from claim 1. As discussed above, Buffam and Matyas fail to form a prima facie case of obviousness of claim 1. It is respectfully submitted that Camp fails to supplement the deficiencies of Buffam and Matyas discussed above, and therefore Buffam, Matyas, and Camp fail to form a prima facie case of obviousness of claim 1. Accordingly, it is respectfully submitted that claims 4, 8, and 9 are allowable at least due to their dependency from claim1.

Further, Applicant notes that Camp is unrelated to the field of the present invention, and indeed unrelated to the field of either Buffam or Matyas. Camp is not in any way related to biometric systems, but is instead related to Global Positioning Systems (GPS). Accordingly, Camp's discussion of determining the location of a user terminal 10 by multiplying a matrix and delta pseudo-ranges to obtain corrections is not applicable to the present invention, or to the feature of claim 4 wherein a code word is generated by generating a matrix.

Similarly, Camp's discussion of calculating distances from satellites to an approximate user location, converting to time of flight, correcting, and "finding the residual of these values modulo 1 millisecond" is not applicable to the present invention, or to the feature of claims 8 and 9 wherein a wherein a modulo n operation is used on creating initial correction data for recovering digitized biometric feature data.

Therefore, it is respectfully submitted that claims 4, 8, and 9 are allowable over the cited references, and withdrawal of the rejection is requested.

Conclusion

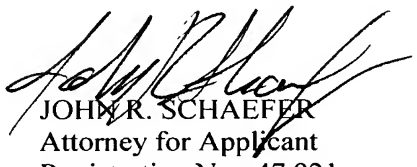
In view of the foregoing remarks, it is respectfully submitted that the application is in condition for allowance. Accordingly, it is requested that claims 1-26 be allowed and the application be passed to issue.

If any issues remain that may be resolved by a telephone or facsimile communication with the Applicant's attorney, the Examiner is invited to contact the undersigned at the numbers shown.

Respectfully submitted,

BACON & THOMAS, PLLC
625 Slaters Lane, Fourth Floor
Alexandria, Virginia 22314-1176
Phone: (703) 683-0500

Date:



JOHN R. SCHAEFER
Attorney for Applicant
Registration No. 47,921